On a Generalised Lehmer Problem for Arbitrary Powers

Igor E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

March 27, 2008

Abstract

We consider a generalisation of the classical Lehmer problem about the parity distribution of an integer and its modular inverse. We use some known estimates of exponential sums to study a more general question of simultaneous distribution of the residues of any fixed number of negative and positive powers of integers in prescribed arithmetic progressions. In particular, we improve and generalise a recent result of Y. Yi and W. Zhang.

1 Introduction

Given modulus $q \geq 2$, we denote by $\mathcal{U}_q$ the set

$$\mathcal{U}_q = \{n \ : \ 1 \leq n < q, \ \gcd(n, q) = 1\}.$$

In particular, $\#\mathcal{U}_q = \varphi(q)$, the Euler function.

For $n \in \mathcal{U}_q$ we use $\overline{n}$ to denote the modular inverse of n, that is, the unique integer $\overline{n} \in \mathcal{U}_q$ with $n\overline{n} \equiv 1 \pmod q$.

The classical question of D. H. Lehmer (see [3, Problem F12]) is about the joint distribution of the parity of n and its modular inverse $\overline{n} \in \mathcal{U}_q$, defined by $n\overline{n} \equiv 1 \pmod q$.

W. Zhang [14, 15] has shown that the Weil bound of Kloosterman sums, see [5, Corollary 11.12], combined with some standard arguments, implies that if q is odd then n and its modular inverse $\overline{n}$ are of the same parity $0.5\varphi(q) + O\left(q^{1/2+o(1)}\right)$ times for $n \in \mathcal{U}_q$.

This result has been extended in generalised in various directions, including its multidimensional analogues, see [1, 2, 6, 7, 9, 10, 11, 12, 13, 14, 15, 16] and references therein.

In particular, it has been shown by Y. Yi and W. Zhang [11], that for any fixed integer $k \neq 0$, the smallest positive residue modulo q of n^k and its modular inverse $\overline{n^k}$ are of the same parity $0.5\varphi(q) + O\left(q^{3/4+o(1)}\right)$ times for $n \in \mathcal{U}_q$.

Here we show that using the bound from [8] of exponential sums with sparse rational functions, one can get the same (as in the case $k = 1$) error term $O\left(q^{1/2+o(1)}\right)$ for any fixed k and in fact obtain an asymptotic formula in a much more general case. Namely given an an integer $s \geq 2$ s-dimensional integer vectors

$$\mathbf{k} = (k_1, \ldots, k_s), \qquad \mathbf{m} = (m_1, \ldots, m_s), \qquad \mathbf{a} = (a_1, \ldots, a_s),$$

where $m_1, \ldots, m_s \geq 1$, we denote by $N_q(\mathbf{m}, \mathbf{a}; \mathbf{k})$ the number of $n \in \mathcal{U}_q$ such that the smallest nonnegative residue of n^{k_j} modulo q is congruent to a_j modulo m_j for every $j = 1, \ldots, s$.

In particular, the result of Y. Yi and W. Zhang [11] can be reformulated as the asymptotic formula,

$$\begin{aligned} N_q\left((2,2),(0,0);(k,k)\right) + N_q\left((2,2),(1,1);(k,k)\right) \\ = \frac{1}{2}\varphi(q) + O\left(q^{3/4+o(1)}\right), \end{aligned} \tag{1}$$

which holds for any odd q.

Here we give the following generalisation and improvement of (1).

Theorem 1. *For any fixed integer $s \geq 2$ and a vector $\mathbf{k} \in \mathbb{Z}^s$ without zero components, uniformly over all vectors $\mathbf{a}, \mathbf{m} \in \mathbb{Z}^s$ with $m_1, \ldots, m_s \geq 1$ and an integer $q \geq 1$ with*

$$\gcd(m_1, q) = \ldots = \gcd(m_s, q) = 1,$$

we have

$$N_q(\mathbf{m}, \mathbf{a}; \mathbf{k}) = \frac{1}{m_1 \ldots m_s}\varphi(q) + O\left(q^{1-1/s+o(1)}\right).$$

In particular, for $s = 2$, $m_1 = m_2 = 2$ and $k_1 = k_2 = k$, Theorem 1 implies that the error term in the asymptotic formula (1) is $O\left(q^{1/2+o(1)}\right)$ for every odd $q \geq 1$.

Throughout the paper, the implied constants in the symbols 'O', and '$\ll$' may depend on the vector $\mathbf{k}$. We recall that the notations $U = O(V)$ and $V \ll U$ are both equivalent to the assertion that the inequality $|U| \leq cV$ holds for some constant $c > 0$.

2 Exponential Sums

For an integer ℓ we denote

$$\mathbf{e}_\ell(z) = \exp(2\pi i z/\ell)$$

and recall that for $u \in \mathbb{Z}$,

$$\frac{1}{\ell} \sum_{-(\ell-1)/2 \leq \mu \leq \ell/2} \mathbf{e}_\ell(\mu u) = \begin{cases} 1 & \text{if } u \equiv 0 \pmod{\ell}, \\ 0 & \text{otherwise,} \end{cases} \tag{2}$$

(which follows immediately from the formula for the sum of a geometric progression).

We also recall that for any integers $U \geq 1$ and μ with $0 < |\mu| \leq \ell/2$ we have

$$\left| \sum_{u=0}^{U} \mathbf{e}_\ell(\mu u) \right| \ll \min\left\{ U, \frac{\ell}{|\mu|} \right\},$$

see [5, Bound (8.6)]. In particular

$$\sum_{\substack{-(\ell-1)/2 \leq \mu \leq \ell/2 \\ \mu \neq 0}} \left| \sum_{u=0}^{U} \mathbf{e}_\ell(\mu u) \right| \ll \ell \log \ell \tag{3}$$

and

$$\sum_{-(\ell-1)/2 \leq \mu \leq \ell/2} \left| \sum_{u=0}^{U} \mathbf{e}_\ell(\mu u) \right| \ll U + \ell \log \ell. \tag{4}$$

Finally, as we have mentioned, our main tool is the following slight generalisation of [8, Theorem 1] which gives an estimate of exponential sums

with sparse rational functions. We note that in [8, Theorem 1] only the case of $d = 1$ has been considered, but the extension to the case of arbitrary d is straightforward.

Lemma 2. *For any fixed integer $s \geq 2$ and a vector $\mathbf{k} \in \mathbb{Z}^s$ without zero components and an integer $q \geq 1$, the bound*

$$\sum_{n \in \mathcal{U}_q} \mathbf{e}_q\left(\sum_{1 \leq j \leq s} \lambda_j n^{k_j}\right) \ll d^{1/s} q^{1-1/s+o(1)}$$

holds, uniformly over all integers $\lambda_1, \ldots, \lambda_s$ with

$$\gcd(\lambda_1, \ldots, \lambda_s) = d.$$

Proof. Let

$$q = \prod_{i=1}^{\nu} p_i^{\alpha_i}$$

be the prime number factorization of q and $q_i = q/p_i^{\alpha_i}$, $i = 1, \ldots, \nu$. We now define t_i as the modular inverse of q_i modulo $p_i^{\alpha_i}$, that is,

$$t_i q_i \equiv \pmod{p_i^{\alpha_i}} \qquad \text{and} \qquad 0 \leq t_i < p_i^{\alpha_i},$$

for $i = 1, \ldots, \nu$. Using the multiplicative property of exponential sums with rational functions, see [5, Equation (12.21)] or [8, Lemma 6], we obtain

$$\sum_{n \in \mathcal{U}_q} \mathbf{e}_q\left(\sum_{1 \leq j \leq s} \lambda_j n^{k_j}\right) = \prod_{i=1}^{\nu} \sum_{n \in \mathcal{U}_{p_i^{\alpha_i}}} \mathbf{e}_{p_i^{\alpha_i}}\left(t_i \sum_{1 \leq j \leq s} \lambda_j n^{k_j}\right). \tag{5}$$

Furthermore, by [8, Lemma 5] we have

$$\sum_{n \in \mathcal{U}_{p^\alpha}} \mathbf{e}_{p^\alpha}\left(\sum_{1 \leq j \leq s} \mu_j n^{k_j}\right) \ll p^{\alpha(1-1/s+o(1))} \tag{6}$$

for any prime power p^α with $p^\alpha \to \infty$ and integers $\mu_1, \ldots, \mu_s$ with

$$\gcd(\mu_1, \ldots, \mu_s, p) = 1.$$

Combining (5) with (6) and using that

$$\nu \ll \frac{\log q}{\log \log q}$$

(which follows from the obvious inequality $\nu! \leq q$ and the Stirling formula) we obtain the result. □

2.1 Proof of Theorem 1

Without loss of generality we may assume that $\mathbf{a}$ has a nonnegative components satisfying $0 \le a_j < m_j$, $j = 1, \ldots, s$.

Let us define U_j as the largest integers U with $m_j U + a_j < q$, $j = 1, \ldots, s$.

Then $N_q(\mathbf{m}, \mathbf{a}; \mathbf{k})$ is equal to the number of solutions to the following system of congruences

$$n^{k_j} \equiv m_j u_j + a_j \pmod q, \quad n \in \mathcal{U}_q,\ 0 \le u_j \le U_j,\ j = 1, \ldots, s. \tag{7}$$

Since $\gcd(m_1 \ldots m_s, q) = 1$, for every $j = 1, \ldots, s$ we consider the moduluar inverse $r_j = \overline{m_j}$ of m_j modulo q, and also define $b_j \in \mathcal{U}_q$ by the congruence $b_j \equiv a_j r_j \pmod q$. Therefore, the system (7) is equivalent to the the following system of congruences

$$r_j n^{k_j} \equiv u_j + b_j \pmod q, \quad n \in \mathcal{U}_q,\ 0 \le u_j \le U_j,\ j = 1, \ldots, s. \tag{8}$$

Using (2) we write

$$\begin{aligned} N_q(\mathbf{m}, \mathbf{a}; \mathbf{k}) &= \sum_{n \in \mathcal{U}_q} \sum_{0 \le u_1 \le U_1} \ldots \sum_{0 \le u_s \le U_s} \\ &\qquad \frac{1}{q^s} \sum_{-(q-1)/2 \le \lambda_1, \ldots, \lambda_s \le q/2} \mathbf{e}_q\left(\sum_{1 \le j \le s} \lambda_j (r_j n^{k_j} - u_j - b_j)\right). \end{aligned}$$

Changing the order of summation and then separating the main term

$$\frac{\#\mathcal{U}_q U_1 \ldots U_s}{q^s} = \frac{\varphi(q) U_1 \ldots U_s}{q^s}$$

corresponding to $\lambda_1 = \ldots = \lambda_s = 0$, we obtain

$$\begin{aligned} N_q(\mathbf{m}, \mathbf{a}; \mathbf{k}) &- \frac{\varphi(q) U_1 \ldots U_s}{q^s} \\ &= \frac{1}{q^s} \sideset{}{^*}\sum_{-(q-1)/2 \le \lambda_1, \ldots, \lambda_s \le q/2} \mathbf{e}_q\left(-\sum_{1 \le j \le s} \lambda_j b_j\right) \\ &\qquad \sum_{n \in \mathcal{U}_q} \mathbf{e}_q\left(\sum_{1 \le j \le s} \lambda_j r_j n^{k_j}\right) \\ &\qquad \sum_{0 \le u_1 \le U_1} \ldots \sum_{0 \le u_s \le U_s} \mathbf{e}_q\left(-\sum_{1 \le j \le s} \lambda_j u_j\right). \end{aligned}$$

where Σ^* means that the term corresponding to $\lambda_1 = \ldots = \lambda_s = 0$ is excluded from the summation. Therefore,

$$\left|N_q(\mathbf{m}, \mathbf{a}; \mathbf{k}) - \frac{\varphi(q)U_1 \ldots U_s}{q^s}\right| \leq \frac{1}{q^s} \sideset{}{^*}\sum_{-(q-1)/2 \leq \lambda_1, \ldots, \lambda_s \leq q/2} \left|\sum_{n \in \mathcal{U}_q} \mathbf{e}_q\left(\sum_{1 \leq j \leq s} \lambda_j r_j n^{k_j}\right)\right| \prod_{1 \leq j \leq s} \left|\sum_{0 \leq u_j \leq U_j} \mathbf{e}_q\left(\lambda_j u_j\right)\right|.$$

Now, for every divisor $d \mid q$ we collect together the terms with the same value of $\gcd(\lambda_1, \ldots, \lambda_s) = d$ and then apply Lemma 2, obtaining the estimate

$$\left|N_q(\mathbf{m}, \mathbf{a}; \mathbf{k}) - \frac{\varphi(q)U_1 \ldots U_s}{q^s}\right| \leq q^{-s+1-1/s+o(1)} \sum_{\substack{d \mid q \\ q<q}} d^{1/s} \Sigma_d, \tag{9}$$

where

$$\Sigma_d = \sum_{\substack{-(q-1)/2 \leq \lambda_1, \ldots, \lambda_s \leq q/2 \\ \gcd(\lambda_1, \ldots, \lambda_s) = d}} \prod_{1 \leq j \leq s} \left|\sum_{0 \leq u_j \leq U_j} \mathbf{e}_q\left(\lambda_j u_j\right)\right|.$$

Writing $\lambda_j = d\mu_j$, $j = 1, \ldots, s$, and $q = dq_d$, we derive

$$\Sigma_d = \sum_{\substack{-(q_d-1)/2 \leq \mu_1, \ldots, \mu_s \leq q_d/2 \\ \gcd(\mu_1, \ldots, \mu_s) = 1}} \prod_{1 \leq j \leq s} \left|\sum_{0 \leq u_j \leq U_j} \mathbf{e}_{q_d}\left(\mu_j u_j\right)\right|.$$

Furthermore, we have

$$\Sigma_d \leq \sum_{1 \leq j \leq s} \sigma_{d,j} \tag{10}$$

where

$$\sigma_{d,j} = \sum_{\substack{-(q_d-1)/2 \leq \mu_1, \ldots, \mu_s \leq q_d/2 \\ \mu_j \neq 0}} \prod_{1 \leq j \leq s} \left|\sum_{0 \leq u_j \leq U_j} \mathbf{e}_{q_d}\left(\mu_j u_j\right)\right|, \qquad j = 1, \ldots, s.$$

We have,

$$\sigma_{d,j} = \sum_{\substack{-(q_d-1)/2\le\mu_j\le q_d/2\\ \mu_j\neq 0}} \left|\sum_{0\le u_j\le U_j} \mathbf{e}_{q_d}(-\mu_j u_j)\right| \prod_{\substack{1\le h\le s\\ h\neq j}} \sum_{-(q_d-1)/2\le\mu_h\le q_d/2} \left|\sum_{0\le u_h\le U_h} \mathbf{e}_{q_d}(\mu_h u_h)\right|.$$

Applying (3) to the sum over μ_j and (4) to the other sums (and using the trivial estimate $U_h \le q$), we obtain

$$\sigma_{d,j} \le (q_d \log q_d) \prod_{\substack{1\le h\le s\\ h\neq j}} (U_h + q_d \log q_q) \le q_d q^{s-1} (\log q_d)^s = d^{-1} q^{s+o(1)}$$

for every $j = 1, \dots, s$. Substituting this in (10), and then recalling (9), we obtain

$$\left|N_q(\mathbf{m}, \mathbf{a}; \mathbf{k}) - \frac{\varphi(q) U_1 \dots U_s}{q^s}\right| \le q^{1-1/s+o(1)} \sum_{\substack{d|q\\ q<q}} d^{-1+1/s} \le q^{1-1/s+o(1)} \sum_{d|q} 1.$$

By the well-known estimate on the divisor function,

$$\sum_{d|q} 1 = q^{o(1)}$$

see [4, Theorem 317], we obtain

$$\left|N_q(\mathbf{m}, \mathbf{a}; \mathbf{k}) - \frac{\varphi(q) U_1 \dots U_s}{q^s}\right| \le q^{1-1/s+o(1)}.$$

It remains to notice that $U_j = q/m_j + O(1)$, $j = 1, \dots, s$. Therefore

$$U_1 \dots U_s = \frac{q^s}{m_1 \dots m_s} + O(q^{s-1}),$$

which concludes the proof.

References

[1] E. Alkan, F. Stan and A. Zaharescu, 'Lehmer k-tuples', *Proc. Amer. Math. Soc.*, **134** (2006), 2807–2815.

[2] C. Cobeli and A. Zaharescu, 'Generalization of a problem of Lehmer', *Manuscr. Math.*, **104** (2001), 301–307.

[3] R. K. Guy, *Unsolved problems in number theory*, Springer-Verlag, New York, 1994.

[4] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, Oxford, 1979.

[5] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[6] H. N. Liu and W. Zhang,'On a problem of D. H. Lehmer', *Acta Math. Sinica*, **22** (2006), 61–68.

[7] S. R. Louboutin, J. Rivat and A. Sárközy', 'On a problem of D. H. Lehmer', *Proc. Amer. Math. Soc.*, **135** (2007), 969–975.

[8] I. E. Shparlinski, 'On exponential sums with sparse polynomials and rational functions', *J. Number Theory*, **60** (1996), 233–244.

[9] I. E. Shparlinski, 'On a generalisation of a Lehmer problem', *Preprint*, 2006 (available from `http://arxiv.org/abs/math/0607414`).

[10] Z. Xu and W. Zhang, 'On a problem of D. H. Lehmer over short intervals', *J. Math. Anal. Appl.*, **320** (2006), 756–770.

[11] Y. Yi and W. Zhang, 'On the generalization of a problem of D. H. Lehmer', *Kyushu J. Math.*, **56** (2002), 235–241.

[12] W. Zhang, Z. Xu and Y. Yi, 'A problem of D. H. Lehmer and its mean square value formula', *J. Number Theory*, **103** (2003), 197–213.

[13] T. Zhang and W. Zhang, 'A generalization on the difference between an integer and its inverse modulo q, II', *Proc. Japan Acad. Sci., Ser.A*, **81** (2005), 7–11.

[14] W. Zhang, 'On a problem of D. H. Lehmer and its generalization', *Compos. Math.*, **86** (1993), 307–316.

[15] W. Zhang, 'On a problem of D. H. Lehmer and its generalization, II', *Compos. Math.*, **91** (1994), 47–56.

[16] W. Zhang, 'On a problem of D. H. Lehmer and Kloosterman sums', *Monatsh. Math.*, **139** (2003), 247–257.